DETAILED ACTION

1. The request filed on October 03, 2008 for a request for continued examination (RCE) under 37 CFR 1.114 based on patent application 10/699,834 is acceptable and an RCE has been established.

2. On December 15, 2008 Examiner and Applicant's representative William H. Bollman, Registration No. 36,457 conducted a telephone interview and discussed the independent claims in view of the prior art on the record. As the result of the interview both parties have agreed to make the following Examiner's amendment. (The subject matter discussed, interview summary, has been attached.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with William H. Bollman, Registration No. 36,457 on 12/16/2008.

The application has been amended as follows: In the claims

28. (Currently Amended) A method of cloaking encrypted data, comprising:

receiving one of voice over IP (VoIP) data, voice over frame relay (VoFR), or voice over ATM (VoATM) data routed by a data router adapted to output a serial data stream;

encrypting said serial data stream into encrypted data using a Type 1 encryption unit;

encapsulating ~~a serial data stream of~~ said encrypted data into IP packets;

forming a first tunnel for an overall IP link;

forming a second tunnel between a first IP encapsulator and a second IP encapsulator; and

transmitting said IP packets of encrypted data on a public IP network.

32. (canceled)

33. (Currently amended) The method of cloaking encrypted data according to claim 28 [[32]], wherein said Type 1 encryption unit comprises:

a KIV type encryption unit.

34. (Currently Amended) The method of cloaking encrypted data according to claim 34 [[33]], wherein said Type 1 KIV-type encryption unit comprises:

a KIV-7 encryption unit.

35. (canceled)

36. (Currently amended) The method of cloaking encrypted data according to claim 28, wherein:

said ~~serial~~ data ~~stream~~ is a synchronous serial data stream.

38. (Currently amended) The method of cloaking encrypted data according to claim 28, further comprising:

combining data from two voice sources into said ~~serial~~ routed data ~~stream before said encapsulation~~.

39. (Currently amended) Apparatus for cloaking encrypted data in a deployable, secure communication terminal, comprising:

means for receiving one of voice over IP (VoIP) data, voice over frame relay (VoFR), or voice over ATM (VoATM) data routed by a data router adapted to output a serial data stream;

means for encrypting said serial data stream into encrypted data using a Type 1 encryption unit;

means for encapsulating ~~a serial data stream of~~ said encrypted data into IP packets;

means for forming a first tunnel for an overall IP link; and

means for forming a second tunnel between a first IP encapsulator and a second IP encapsulator; and

means for transmitting said IP packets of encrypted data on a public IP network.

43. (canceled)

46. (canceled)

47. (Currently amended) The apparatus for cloaking encrypted data in a deployable, secure communication terminal according to claim 39, wherein:
said ~~serial~~ data ~~stream~~ is a synchronous serial data stream.

49. (Currently amended) The apparatus for cloaking encrypted data in a deployable, secure communication terminal according to claim 39, further comprising:

means for combining data from two voice sources into said ~~serial~~ routed data ~~stream before said means for encapsulating encapsulates said serial data stream~~.

51. (proposed amended) A secure communications device, comprising:

means for receiving one of voice over IP (VoIP) data, voice over frame relay (VoFR), or voice over ATM (VoATM) data stream routed by a data router adapted to output a serial data stream;

means for encrypting [[a]] said serial data stream using a Type 1 encryption unit, into an encrypted data stream;

means for encapsulating said encrypted data stream for transmission to another secure communications device using IP protocol; ~~and~~

means for forming a first tunnel for an overall IP link; ~~and~~

means for forming a second tunnel between a first IP encapsulator and a second IP encapsulator; and

means for routing said encapsulated, encrypted data stream over an Internet.

Allowable Subject Matter

3. **Claims 28-31, 33-34, 36-42, 44-45 and 47-54** are allowed.

4. The following is an examiner's statement of reasons for allowance:

5. Referring to **independent claims 28, 39 and 51, the combination of the reference namely Nortel, Gross and Francisco , discloses some of the limitation recited above.**

For instance,

Nortel discloses a method of Cloaking an encrypted serial data stream [See figure 1 and 2 and page 3, 1st column) comprising:

Receiving a voice stream from a telephony device at a data router adapted to output a first serial data stream *[See figure 1 and 2 and page 2, column 2]*

said data router being further adapted to receive any of voice-over-IP (VolP), [*[See figure 1 and 2 and page 2, column 2]*

Encrypting said voice stream into a second serial data stream;

encapsulating said second serial data stream of encrypted data into Internet Protocol (IP) packets; [Page 2, column 3, 1st paragraph, see also figure 2, "Encrypted Voice/data"]and

Transmitting said IP packets of encrypted serial data on a public IPnetwork [See figure 1, "Public IP network"]

Nortel does not explicitly disclose

, said data router being further adapted to receive any of voice-over-IP (VolP), voice-over-frame relay (VoFR), and voice-over-ATM (VoATM) communications;

However, in the same field of endeavor Gross on paragraph 0041 and figure 1-2, ref. Num "20-24" and "4" discloses the above feature.

However, the combination of Nortel and Gross does not explicitly disclose encrypting data using a Type 1 encryption unit

However, in the same field of endeavor Francisco on page 705, paragraph 2.1.2, discloses that the transmission of serial data stream **encrypted with a standard Type I serial encryptor before or prior to entering the GBS system. Furthermore Francisco on** Page 706, paragraph 2.3 discloses that **the internet/**Public IP network service/AKA Asynchronous Networking or Split-IP provides a wide-bandwidth one-way data path over the satellite.

- **However, as applicant persuasively** argued, the combination of the reference **Nortel, Gross and Francisco,** does not disclose the following specific functional limitation which is added/recited in the new independent claims **28, 39 and 51.**

forming a second tunnel between a first IP encapsulator and a second IP encapsulator;

None of the prior art of record taken singularly or in combination teaches a method of cloaking an encrypted serial data stream comprising, the

above functional limitation, together with the other limitation recited in the respective independent claims 28, 39 and 51, and for this reason, independent claims 28, 39 and 51 are found to be novel and are allowed.

Note: For the Apparatus claims 39 and for claim 51, Examiner interpreted the **"data router**" recited in the claims as a hardware unit, such interpretation is given in view of the specification.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submission should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

12/17/2008

/Samson B Lemma/
Examiner, Art Unit 2432

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2432